

Application Service Provider Privacy & Security Policies

Access

Practice Partner ASP customers have had a good experience connecting to our ASP solutions over the Internet. The reason for their success is that our customers have been careful in selecting good ISPs. ISPs offer three different methods of Internet connectivity for small business customers: cable, DSL, and T1. Good internet connectivity is a function of various factors. For the Practice Partner ASP, the most important factors to ensure good Internet connectivity are:

- Appropriate bandwidth for the number of users and expected data transmission
- Low latency
- No packet loss

Bandwidth is easiest to acquire and widely marketed by the different ISPs. However, the factors that most negatively affect our customers are when latency is higher than expected or when packet loss occurs. In these situations, the application the customer is using is not available or unresponsive. This negative experience typically occurs when using cable or DSL and is rarely seen with T1. This is because ISPs offer a higher service level agreement (SLA) to T1 customers than they offer to cable or DSL customers.

In determining which ISP to use, please consider the following factors when making your decision.

Appropriate Bandwidth – The amount of bandwidth a user needs depends on the amount of data being requested at any particular time. Some tasks result in transmitting more data across the ASP. For example, uploading scanned images, viewing scanned images or printing long reports increases the amount of data being transmitted. If the amount of bandwidth is not sufficient, the result will be increased latency and possibly packet loss.

# of Workstations	Bandwidth w/o daily scanning	Bandwidth w/ daily scanning*
1-20	512kbps upload/512kbps download	1024 kbps upload/1024 kbps download
21-40	1024 kbps upload/1024 kbps download	1500 kbps upload/1500 kbps download
More than 40	1500 kbps upload/1500 kbps download	1500 kbps upload/1500 kbps download**

*The increased bandwidth requirements when scanning daily assumes that scanning is occurring throughout the day.

**Sites considering expanding to a second T1 should consult with their ISP.

Low Latency – Latency is the amount of time it takes data to travel between Practice Partner and the user's workstation (and vice-versa). Consistently low latency is optimal for good ASP performance. For acceptable usage, we require that latency hardly ever exceed 120 milliseconds latency during work hours (using a ping utility, 95% of packets should be transmitted within 120 milliseconds and rarely should any result exceed 150 milliseconds).

No Packet Loss – Packet loss can be attributed to extremely high latency or general failures in communication between the client machine and Practice Partner servers. Any amount of packet loss can cause a disruption in ASP service. During work hours, packet loss should not last for more than 5 seconds and should be a rare occurrence. Ideally, there is no packet loss.

Recommendation – Practice Partner strongly recommends that customers ensure that their ISP

	is able to meet the above Internet connectivity requirements. Using a fractional or full T1 connection is the optimal solution if available at a reasonable cost, especially if using Total Practice Partner solution with our Zoom scanning product. Some of our customers have reported that by bundling Internet and telephone over a T1, they experienced significant cost savings. Customers who wish to use DSL or cable are advised that if the DSL or cable connection does not meet the requirements above, they will need to switch to a T1 or fractional T1.
Authorization	Because we utilize 128 bit SSL encryption and Virtual Private Network (VPN) technology, data communication travels through a secured pathway to and from each customer. The VPN connections are encrypted using 3DES encryption and authenticated using RSA's SecurID token system. Office connections are encrypted using 128 bit SSL certificates. Practice Partner approved firewalls are required at the office's network. Protection of resources. By using the latest security and networking technology, only confirmed users are granted access to authorized applications.
Authentication	Proof of identity. Practice Partner ASP employs the latest SecurID authentication technology, creating a barrier that is much stronger than a conventional password system. It combines the user's personal identification number (a four digit PIN) with a unique six-digit number that changes every 60 seconds and is specific to the user and the time. Each user is given token (a key-chain sized device) that generates the new codes continuously for three years. Only when the correct PIN and token are entered on the VPN logon screen is access granted. The Practice Partner data center is physically secured behind multiple-card key access points and protected by motion detectors connected to a national security company.
Audit	
Secondary Uses of Data	
Data Ownership	The customer owns the data.